Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	
	)	
	)	

To: The Commission

REPLY COMMENTS OF CENTURYLINK, INC.

Kathryn Marie Krause
Associate General Counsel
CENTURYLINK, INC.
1099 New York Avenue, NW
Suite 250
Washington, D.C. 20001
(303) 992-2503

Linda K. Gardner
Chief Privacy Officer and
Associate General Counsel
CENTURYLINK, INC.
600 New Century Parkway
New Century, KS 66031
(913) 353-7030

Russell P. Hanser
Joshua M. Bercu
WILKINSON BARKER KNAUER, LLP
1800 M Street, NW, Suite 800N
Washington, D.C. 20036
(202) 783-4141

July 6, 2016

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	
	)	
	)	

To: The Commission

REPLY COMMENTS OF CENTURYLINK, INC.

CenturyLink, Inc. ("CenturyLink") files these reply comments in response to the Notice of Proposed Rulemaking ("*Notice*") in the above-referenced proceeding.[1]

I. INTRODUCTION AND SUMMARY

The record makes clear that the Commission's proposed broadband privacy and data security rules raise many legal, technical, and operational problems. Indeed, myriad commenters – including both Internet service providers ("ISPs") and others – raised concerns about numerous aspects of the proposed approach. For example, ISPs and other ecosystem players showed that the Commission lacks the authority to pursue rules governing categories of information that fall outside the statutory definition of customer proprietary network information ("CPNI").[2] Many of these commenters – most notably the staff of the Federal Trade Commission ("FTC Staff") Bureau of Consumer Protection – also questioned the lawfulness and propriety of a privacy and

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (2016) ("*Notice*").

[2] *See, e.g.*, CenturyLink Comments at 13-14; American Cable Association ("ACA") Comments at 10-21; AT&T Comments at 60-68, 103-110; Consumer Technology Association ("CTA") Comments at 4-6; ITTA Comments at 4-11; National Cable & Telecommunications Association ("NCTA") Comments at 7-28.

data security regime that treated all data alike, regardless of the data's sensitivity.[3] Yet another wide-ranging group of commenters raised concerns about the proposed opt-in regime, with some – including leading constitutional law scholar Laurence H. Tribe – questioning the very constitutionality of the Commission's proposal.[4] CenturyLink and others raised the insurmountable practical concerns associated with the proposed approach.[5] Finally, many commenters expressed concern about the Commission's approach to data security, which imposes a *de facto* "strict liability" regime,[6] and questioned the utility of prescriptive data security rules generally.[7]

Although some parties supported the *Notice*'s proposed approach, these commenters failed to supply meaningful legal, policy, and operational support tied specifically to the proposed rules, relying instead on speculative fears and generic bromides. The record thus

---

[3] *See, e.g.*, FTC Staff Comments at 23; CenturyLink Comments at 16; Cincinnati Bell Telephone Company, LLC ("Cincinnati Bell") Comments at 11; CTIA Comments at 94; CTA Comments at 4-5, 9; Internet Commerce Coalition Comments at 9-10; ITTA Comments at 18-19; NTCA Comments at 8-9; State Privacy and Security Coalition Comments at 4-5; Verizon Comments at 24; *see also* Comments of Former FTC Chairman Jon Leibowitz ("Leibowitz") at 9; FTC Commissioner Maureen K. Ohlhausen ("Ohlhausen") Comments at 1-2; Professor Laurence H. Tribe ("Tribe") Comments at 5.

[4] *See* Tribe Comments at 1-6; *see also, e.g.,* Association of National Advertisers ("ANA") Comments at 31; Comments of CTIA at 12-13, 74-94.

[5] *See, e.g.*, CenturyLink Comments at 20-21; Cincinnati Bell Comments at 13; Competitive Carriers Association ("CCA") Comments at 28-30; Software Information and Industry Association Comments at 9-10.

[6] *See, e.g.*, CenturyLink Comments at 32-36; CTA Comments at 10; T-Mobile USA, Inc. ("T-Mobile") Comments at 47-49; CTIA Comments at 160.

[7] *See, e.g.*, AT&T Comments at 75-79; CenturyLink Comments at 33-34; Cincinnati Bell Comments at 8-9; CCA Comments at 34-38; CTIA Comments at 159-165; Direct Marketing Association ("DMA") Comments at 21-23; Georgetown University Security and Software Engineering Research Center ("SSERC") Comments at 24-25.

largely lacks evidence demonstrating that the Commission has the legal authority to adopt such broad rules, that public policy supports prescriptive privacy and data security rules, or that the benefits of many of the proposed rules outweigh their substantial costs.

This is no coincidence: Supporters of the *Notice* have failed to offer this evidence because they cannot. The record makes clear that the proposed rules, as currently constructed are unlawful, comprise bad policy, and impose undue burdens. Given the lack of compelling support in the record for the Commission's proposed approach, and the range of areas in which the record lacks reasoned support for the *Notice*'s proposals, the Commission cannot lawfully move forward without making significant changes to the proposed rules.

II. THE RECORD LACKS LEGAL SUPPORT FOR THE *NOTICE*'S PROPOSED RULES

The vast majority of commenters who support the *Notice*'s proposal glaringly fail to discuss the Commission's legal authority to adopt it. Those who do discuss the Commission's jurisdiction either offer conclusory trope bereft of legal analysis or rely on flawed arguments that do not support the proposed rules. Some commenters, for example, incorrectly claim that Section 222(a) imposes a standalone duty on telecommunication carriers.[8] However, as CenturyLink and others have demonstrated, Section 222(a) imposes no such independent duty.[9] Indeed, as ITTA explained, the plain language and structure of Section 222, the legislative history of Section 222(a), and, until recently, the Commission's consistent interpretation (*i.e.*,

[8] *See, e.g.*, Center for Democracy & Technology ("CDT") Comments at 8; Greenlining Institute and Media Alliance ("Greenlining") Comments at 50; New America's Open Technology Institute ("OTI") Comments at 41.

[9] *See* CenturyLink Comments at 13-14 (Section 222 limits the FCC's privacy and data security authority to CPNI; the Commission cannot use the general language of Section 222(a) to expand the scope of protected customer information); *see also, e.g.*, Mobile Future Comments at 11-12; NCTA Comments at 14-18.

that Section 222's substantive mandates are limited to CPNI) all demonstrate that Section 222(a) does *not* impose an independent legal duty on carriers to protect information other than CPNI.[10]

Even if the Commission were right, and Section 222(a) conferred on it a duty to protect information beyond CPNI, it could not simply impose a regime based on Section 222(c) – which Congress specifically limited to CPNI – to this larger category of information. Rather, it would follow from the Commission's logic that Congress intended the regulatory treatment of information covered by Section 222(a) (if any) to be different from – and less onerous than – the regulatory treatment of the narrower, and more sensitive, information at issue in Section 222(c). If not, there would have been no reason for Congress to differentiate between CPNI and the information purportedly addressed by Section 222(a) – it simply would have applied subsection (c) to all such information. Of course, Congress did no such thing.

While some commenters claim that Section 222 compels the Commission to act here (because BIAS has been deemed a telecommunications service and Section 222 applies to providers of such offerings),[11] that argument – even if assumed to be correct – would not warrant the specific mandates under consideration. Clearly, there is no legal compulsion to establish rules pursuant to Section 222(a) governing information that is not CPNI – as evidenced by the Commission's choice not to promulgate any such rules (with respect to telephony or other offerings) in the twenty years since Congress enacted Section 222. In short, even if one agreed

[10] ITTA Comments at 3-11.

[11] *See, e.g.*, American Civil Liberties Union Comments at 7 (arguing that Congress intended for Section 222 to extend beyond the telephone network, compelling the Commission to act, as content must be protected); CDT Comments at 2 (arguing that Section 222 must include a broader set of information than CPNI alone).

that Section 222 required adoption of CPNI requirements for BIAS, that would not justify rules extending beyond CPNI via Section 222(a).

III. THE RECORD LACKS A POLICY RATIONALE FOR PRESCRIPTIVE ISP-SPECIFIC PRIVACY AND DATA SECURITY RULES

The claim that ISPs are different from other entities within the Internet ecosystem in ways that warrant unique privacy and data security rules has been thoroughly refuted.[12] Indeed, even the Electronic Privacy Information Center, which supports the Commission's privacy rules as a general matter, has posited that consumers "routinely shift from one ISP to another as they move between home, office, mobile, and open WiFi services" but ultimately end up relying on the same edge providers.[13] Thus EPIC notes, ISPs might well have less visibility into user activities than such edge providers.[14] As CenturyLink and others have explained, increasing use of encryption and VPNs are further limiting ISPs' access to user information.[15]

Some parties continue to claim that ISPs differ from their competitors on the edge in ways that are material here. This is not so. For example, some argue that consumers have more

---

[12] *See, e.g.*, Communications Workers of America ("CWA") Comments at 3 (the notion that ISPs have unique access to sensitive and personal digital information is factually wrong and outdated); Electronic Transactions Association Comments at 6-7 (ISP access to data is neither unique nor comprehensive; other entities have comparable access to customers' online activity); ITIF Comments at 3-6 (the Commission must demonstrate a unique risk of harm to consumers from ISP activity before enacting such prescriptive regulations; it cannot do so, because such a risk does not exist in part thanks to the rise of encryption and VPN usage); Verizon Comments at 16-23 (ISPs do not have unique or comprehensive access to data, nor is their access unavoidable).

[13] Electronic Privacy Information Center ("EPIC") Comments at 16.

[14] *See id.*

[15] *See, e.g.*, CenturyLink Comments at 7-8; American Enterprise Institute for Public Policy Research Comments at 4; Professor Christopher S. Yoo Comments at 4-5; Electronic Transaction Association Comments at 6-7; ITIF Comments at 6-7; Verizon Comments at 16-23.

choices among edge providers than ISPs,[16] but ignore that it may not actually be that easy to switch edge providers. Indeed, as the record demonstrates, the high costs associated with abandoning or migrating long-used social media accounts, email accounts, operating systems, or other edge-provider offerings refute any suggestion that customers only face switching barriers in connection with their ISPs.[17]

Some commenters have claimed that ISPs' access to consumer information "creates many opportunities for abuse and misuse of data."[18] Notably absent from their hypotheticals are concrete examples of instances in which ISPs have in fact abused and misused consumer data in a way that existing protections, including market forces, public pressure, and regulatory oversight, could not address.[19] As CenturyLink previously noted, regulatory agencies and privacy advocates have historically shown greater concern regarding edge providers' practices than the practices of BIAS providers.[20] Moreover, no party has demonstrated, or could demonstrate, that a privacy approach consistent with that of the FTC would fail to protect BIAS

---

[16] *See* Free Press Comments at 4-5; OTI Comments at 5-6.

[17] *See, e.g.,* AT&T Comments at 47 ("[C]onsumers may find it much more difficult to abandon leading edge providers if they dislike some aspect of their privacy policies … switching operating systems typically means switching devices (e.g., replacing an Android-based Samsung with an iOS-based iPhone), and that not only costs money, but often requires the consumer to abandon many of the apps and much of the data on the old phone … social networks are not typically interconnected with one another, which means that the largest ones benefit from enormous network effects … unlike telephone numbers, email addresses are non-portable"); NetCompetition Comments at 15.

[18] *See, e.g.*, OTI Comments at 2-3.

[19] Some parties cite ISPs' privacy policies as evidence of ISP potential misuses of data. *See, e.g.*, CDD Comments. However, these commenters fail to show that misuse is happening, or even that if it were, it could not be addressed by alternate means. *See, e.g.*, Verizon Comments at 43.

[20] *See* CenturyLink Comments at 3 n.5.

consumers.[21] Yet the Commission contemplates a dichotomous framework in which BIAS providers are subject to expansive *ex ante* rules and edge providers are subject only to the FTC's more permissive regime.

In any event, the record is bereft of evidence showing that the proposal is tailored to address anything unique about ISPs or their activities. Instead, commenters only offer up red herrings. For example, Public Knowledge *et al.* appear to conflate deep packet inspection ("DPI") – and access to the *content* of broadband transmissions – with other ways in which BIAS providers may obtain data from customers. They assert that implementing a regime based on the sensitivity of the data "in the broadband context is not feasible, as it would necessarily require ISPs to first determine whether sensitive information is present in any given communication – a task necessarily requiring *manual inspection of each packet – before* applying the appropriate amount of protection."[22] This assertion is simply not true, as it assumes that the *Notice* only addresses information that BIAS providers transport on behalf of their customers, when in fact it also addresses information that could be discerned and understood without the use of DPI.

But the *Notice* is substantially broader than suggested by Public Knowledge *et al.* The proposed rules, if adopted without change, would address *all* of the information a BIAS provider holds about its customers, regardless of how it is collected. Thus, the proposed rules would cover information whose sensitivity is easily ascertained without any review of the content of the user's communications. And arguments such as that made by the National Consumers League

[21] There is widespread agreement that the FTC's approach to privacy has served consumers well. *See, e.g.*, FTC Staff Comments at 3-6; Leibowitz Comments at 2-7; Ohlhausen Comments at 1-3. Any commenters who argue the contrary – and few do, at least with any significant intellectual rigor – would have to blatantly disregard the massive advantages to consumers that the Internet has granted during its growth under FTC stewardship.

[22] Public Knowledge *et al.* Comments at 24 (emphasis in original).

that "all information held by BIAS providers is sensitive" because of BIAS providers' purported access to vast troves of customer data and an alleged absence of broadband competition fail given the makeup of the Internet ecosystem[23] Even if, *arguendo*, these assertions were true, they still could not justify treating data that poses little risk of harm to consumers, including data widely available across the Internet infrastructure, as "sensitive" solely because of the identity of the entity holding the data.[24]

In sum, the record simply does not and cannot support ISP-specific privacy rules that are far more restrictive than those that apply to the rest of the Internet ecosystem.

IV. THE RECORD PROVIDES NO REASON TO BELIEVE THAT THE PROPOSAL'S BENEFITS WOULD OUTWEIGH ITS COSTS

The record demonstrates that the *Notice*'s proposal would impose real costs to both consumers (*e.g.*, in confusion and higher costs)[25] and providers (*e.g.*, in compliance costs),[26] but includes little to no discussion showing that the benefits would exceed (and thus might justify) these costs. In particular, the record makes clear that (1) a restrictive *ex ante* approach to privacy and data security, (2) the proposed opt-in regime, (3) the overbroad data breach obligation, and (4) a strict liability approach to data security would each fail even the most rudimentary cost-benefit analysis.

---

[23] National Consumers League Comments at 9.

[24] *See, e.g.*, AT&T Comments at 38; CenturyLink Comments at 35; CWA Comments at 3; ITIF Comments at 3-4.

[25] *See, e.g.*, ACA Comments at 57; CTIA Comments at 116, 179; Free State Foundation Comments at 7-8; Hughes Network Systems, LLC Comments at 3; ICLE and Scholars of Law & Economics Comments at 15-16.

[26] *See, e.g.*, CALinnovates Comments at 6-7; CenturyLink Comments at 45; NCTA Comments at 83-84.

Prescriptive* Ex Ante *Approach. The record fails to demonstrate why prescriptive *ex ante* privacy rules protect consumers better than a principles-based *ex post* approach such as that utilized by the FTC. To the contrary, the record demonstrates the substantial costs that *ex ante* privacy rules impose on competition and innovation.[27] As CALinnovates describes, the Commission's proposed framework would discourage privacy innovation that could occur in the absence of increased compliance burdens.[28] Likewise, the George Washington University Regulatory Studies Center observes that an *ex post* enforcement regime, such as the FTC's, largely avoids artificial barriers to competition and innovation.[29]

While the record details the costs of an *ex ante* approach to privacy, it lacks evidence demonstrating any clear *benefits* of such an approach. At most, advocates offer high-level assertions regarding speculative and unsubstantiated concerns about ISPs' practices and capabilities.[30] They do not explain why a predictable and fair *ex post* enforcement approach is insufficient to protect consumers, or why the FTC's successful approach has not worked and/or

---

[27] *See, e.g.*, Citizens Against Government Waste Comments at 2 (switching from *ex post* FTC enforcement to prescriptive *ex ante* FCC regulations would adversely affect innovation and consumers); CTA Comments at 12 (arguing that at most, the FCC should adopt an *ex post* approach consistent with that of the FTC, which requires "reasonable data security safeguards" and is designed to be flexible – specifically, "to permit and encourage innovation").

[28] CALinnovates Comments at 6-7.

[29] George Washington University Regulatory Studies Center Comments at 2-3.

[30] *See, e.g.*, Public Knowledge *et al.* Comments at 3 (asserting that "BIAS providers are gatekeepers to the Internet" and claiming "[t]his position is unique to BIAS providers and carries substantial implications for consumers"); OTI Comments at 3-4 (claiming that at "a technical level, ISPs have a wide range of ways to gather and compile an extremely detailed profile about each subscriber" while citing with a broken link to a separate document that also fails to sufficiently explain how).

would not work for BIAS.[31] Notably, the FTC staff explains that this approach does protect consumers, noting that the "FTC's ongoing enforcement actions – in both the physical and digital worlds – send an important message to companies about the need to protect consumers' privacy and data security."[32] This framework would ultimately serve consumers better than the prescriptive *ex ante* rules under consideration here.

Opt-In Regime. Relatedly, the record lacks evidence that an opt-in approach better protects consumers than an opt-out approach, or that the costs an opt-in approach would impose on business operations and consumers – costs clearly demonstrated in the record – are justified by any purported-but-unproven "protection" afforded by opt-in consent requirements.[33] Instead, as the staff of the FTC explained, an approach that "does not reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data … could hamper beneficial uses of data that consumers may prefer, while failing to protect against practices that

[31] Indeed, as noted above, advocates disclaiming the success of the FTC's regime seem to willfully ignore the fact that the consumer-friendly Internet services they ostensibly seek to safeguard emerged in an era of FTC oversight.

[32] FTC Staff Comments at 5.

[33] *See, e.g.*, Advanced Communications Law & Policy Institute Comments at 16 (adopting an opt-in regime for ISPs would hamper the ability of ISPs to compete with digital advertisers such as Facebook and Google); ANA Comments at 15, 26 (noting that requiring opt-in consent for most third-party users of data would detrimentally change the entire process of consent for a whole segment of adherents to the self-regulatory programs, and that no other U.S. online privacy framework requires companies to obtain opt-in consent for uses of non-sensitive information); AT&T Comments at 53-55 (an asymmetrical opt-in regime would raise broadband prices and dampen broadband investment incentives, and chill innovation while suppressing competition); CCA Comments at 25-26 (arguing that the proposal requiring ISPs to solicit and receive opt-in customer approval should be rejected, particularly in light of the costs that providers would incur); CTA Comments at 8 (arguing that requiring ISPs to obtain opt-in consent for most uses and disclosers of any type of customer information will lead to absurd results).

are more likely to be unwanted and potentially harmful."[34] Fundamentally, the proposed opt-in regime would actually disserve consumers.[35]

Breach Notification. CenturyLink and others have advocated that any breach notification requirement should apply only where there is a potential for actual customer harm.[36] Some commenters assert that such a harm-based trigger would prevent customers from assessing the impact of a given data breach, and acting as they see appropriate.[37] Others argue that a harm-based trigger would insulate BIAS providers from the negative consequences that might otherwise result from notification – for example, reputational harms – if the public became aware of the number of instances in which there had been any unauthorized access to customer data.[38] Such arguments are patently illogical. First, they fail to demonstrate any sound economic, social, or consumer protection basis for encouraging customers to "protect themselves" from activities where there is no likelihood of *actual* harm to such customers (*i.e.*, cases that would not satisfy a threshold harm-based trigger). Second, they also fail to address, let alone overcome, the ways in which overnotification would independently confuse and burden consumers – creating an

[34] FTC Staff Comments at 22.

[35] *See, e.g.,* Joshua D. Wright, *An Economic Analysis of the FCC's Proposed Regulation of Broadband Privacy* at 20-28 (May 27, 2016) (finding that the opt-in regime would raise retail broadband prices, impose indirect consumer harms, and hamper innovation and experimentation), attached to USTelecom Ex Parte (May 27, 2016).

[36] *See, e.g.*, CenturyLink Comments at ii, 40-44; Advanced Communications Law & Policy Institute Comments at 19; CCA Comments at 44-45.

[37] *See, e.g.*, American Association for Justice Comments at 7; National Consumers League Comments at 24-25.

[38] *See* OTI Comments at 42.

entirely new collateral harm as a result. As the FTC staff has described, the *Notice*'s broad breach notification proposal raises two concerns:

> The first concern is that because the definition [of breach] includes unauthorized access to *any* customer proprietary information, companies that only collect data such as device identifiers or information held in cookies may be required to collect *other* consumer information such as email addresses in order to provide consumers with breach notification. … A second concern is overnotification.[39]

That these concerns are expressed by the agency the U.S. government holds forth to the world as a paramount guardian of consumer privacy is most telling, and should prompt the Commission to rethink the purported benefits of its overly broad proposed notification requirement and ultimately to reject it. As written, that requirement stands to harm consumers and impose unnecessary burdens on ISPs – all without generating any actual benefit for consumers.

Data Security. Although the Commission purports to espouse a data security standard based on "reasonableness" and consistent with the FTC's approach, the actual language of the proposed rule contemplates a strict liability framework, obliging ISPs to "ensure" data security under any and all circumstances.[40] No commenter asserts, nor could assert, that a strict liability approach to data security ultimately would justify its tremendous and problematic costs. As the FTC staff explains, an approach to data security focused on "reasonable data security practices – with an emphasis on risk management – instead of enumerating particular technological measures … protects consumers from lax data security practices, while also giving businesses

[39] FTC Staff Comments at 31.

[40] *See* CenturyLink Comments at 32; *see also* CCA Comments at 38; CTA Comments at 10; CTIA Comments at 159; ITTA Comments at 23; T-Mobile Comments at 47-48.

the flexibility to tailor their programs to their particular circumstances."[41] In contrast, a strict liability approach is both infeasible and unreasonable, and would impose substantial costs and cause unintended consequences as ISPs misallocate resources in ways that do not better protect their customers.[42] The Commission should rethink its strict liability approach to data security, and instead allow ISPs the flexibility to adopt appropriate and reasonable data security safeguards based on the given ISPs' needs, capabilities, and practices.

V. CONCLUSION

CenturyLink again urges the Commission to reconsider many of the proposals set forth in the *Notice*, which are unsupported by the record. Instead, a broadband privacy regime consistent with the FTC's successful approach to privacy – including, for example, one based on the proposal set forth by a coalition of industry associations[43] – would protect consumer privacy while also better serving consumers, competition, and the public interest.

[41] FTC Staff Comments at 27.

[42] *See, e.g.*, CenturyLink Comments at 33-36; AT&T Comments at 79; CTA Comments at 10; CTIA Comments at 159-160; T-Mobile Comments at 47-48.

[43] *See* Letter from Matthew M. Polka, Steven K. Berry, Meredith Attwell Baker, Michael Powell, and Walter M. McCormick, Jr. to Tom Wheeler, Chairman, FCC (Mar. 1, 2016), https://www.ustelecom.org/sites/default/files/documents/Wheeler%20Letter%20Re%20Privacy%20Principles%203%201%2016%20%283%29.pdf; *see also* CenturyLink Comments at 4-5.

Respectfully submitted,

CENTURYLINK, INC.

/s/
Russell P. Hanser
Joshua M. Bercu
WILKINSON BARKER KNAUER, LLP
1800 M Street, NW, Suite 800N
Washington, D.C. 20036
(202) 783-4141

Its Attorneys

Kathryn Marie Krause
Associate General Counsel
CENTURYLINK, INC.
1099 New York Avenue, NW
Suite 250
Washington, D.C. 20001
(303) 992-2503

Linda K. Gardner
Chief Privacy Officer and
Associate General Counsel
CENTURYLINK, INC.
600 New Century Parkway
New Century, KS 66031
(913) 353-7030

June 27, 2016